Team CyberData's Support for Upcoming NOAA Requirements

Below are upcoming NOAALink Enterprise initiatives that may be issued for bid as listed on the NOAALink webpage (3/6/12). Listed below each initiative are Team CyberData's past performance references showing how we are currently supporting or have supported similar efforts in the past. To the best of our understanding, we've listed references that we believe are similar in nature to the referenced initiative. As we learn more about each potential task order we will update the information accordingly. By pressing the CTRL and clicking a reference you will jump to the selected reference.

Requirement Title: IT and Administrative Services Contract
Line/Staff Office: NWS, National Centers for Environmental Prediction

Relevant Past Performance Experience

- (PPR5) NOAA/NWS Office of Hydrologic Development IT Infrastructure Support
- (PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development
- (PPR4) Department of the Treasury Application Support Services Contract

Requirement Title: NODC Scientific Data Management Support Services
Line/Staff Office: NESDIS

Relevant Past Performance Experience

- (PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development
- (PPR4) Department of the Treasury Application Support Services Contract
- (PPR7) NOAA/NOS GIS and Web Consulting, Electronic Navigational Chart (ENC) Quality Assurance

Requirement Title: Microsoft Enterprise Agreement
Line/Staff Office: NWS, Office of Chief Information Officer

CyberData does not intend to Bid

Requirement Title: NextGen Security Support
Line/Staff Office: NESDIS

Relevant Past Performance Experience

- (PPR1) NOAA/NWS Dissemination Systems Branch and Telecommunication Gateway Support
- (PPR2) NOAA Computer Incident Response Team Security Office (CIRT)
- (PPR3) Support for the Department of Homeland Security

Requirement Title: NMFS Alaska Region Technical Support Application Development Services
Line/Staff Office: NMFS

Relevant Past Performance Experience

- (PPR8) NOAA/NMFS, Science Information Management and Scientific Research Information Technology
- (PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development
- (PPR4) Department of the Treasury Application Support Services Contract
- (PPR7) NOAA/NOS GIS and Web Consulting, Electronic Navigational Chart (ENC) Quality Assurance

Requirement Title: NCEP IT Support Services
Line/Staff Office: NWS, National Centers for Environmental Prediction

Relevant Past Performance Experience

- (PPR1) NOAA/NWS Dissemination Systems Branch and Telecommunication Gateway Support
- (PPR9) Department of Commerce Information Technology, Help Desk Support Services
- (PPR8) NOAA/NMFS Science Information Management and Scientific Research Information Technology
- (PPR5) NOAA/NWS Office of Hydrologic Development IT Infrastructure Support

Requirement Title: IT Support Services
Line/Staff Office: NOS, Office of Chief Information Officer

Relevant Past Performance Experience

- (PPR1) NOAA/NWS Dissemination Systems Branch and Telecommunication Gateway Support
- (PPR2) NOAA Computer Incident Response Team Security Office (N-CIRT)
- (PPR4) Department of the Treasury Application Support Services Contract
- (PPR5) NOAA/NWS Office of Hydrologic Development IT Infrastructure Support
- (PPR7) NOAA/NOS, GIS and Web Consulting, Electronic Navigational Chart (ENC) Quality Assurance
- (PPR9) Department Of Commerce, Information Technology Help Desk Support Services
- (PPR10) GSA Consolidated Information System – ROCIS III
- (PPR11) General Services Administration, Public Buildings Services

Requirement Title: Conversion & Upgrade of Marine Mammal Systems
Line/Staff Office: NMFS, Office of Protected Resources

Relevant Past Performance Experience

- (PPR10) GSA Consolidated Information System – ROCIS III

Requirement Title: Legacy SW product in Oracle Forms migration to APEX
Line/Staff Office: NMFS, NMFS/OMB/MB5

Relevant Past Performance Experience

- (PPR10) GSA Consolidated Information System – ROCIS III

Requirement Title: NOAA Cyber Security Center Support
Line/Staff Office: Office of Chief Information Officer, IT Security Support

Relevant Past Performance Experience

- (PPR1) NOAA/NWS Dissemination Systems Branch and Telecommunication Gateway Support
- (PPR2) NOAA Computer Incident Response Team Security Office (CIRT)
- (PPR3) Support for the Department of Homeland Security programs

Requirement Title: Grants Online Operations and Maintenance
Line/Staff Office: Office of Chief Information Officer, Administrative Systems Management Division

Relevant Past Performance Experience

- (PPR13) NOAA Grants Online (GOL)
- (PPR4) Department of the Treasury Application Support Services Contract

Requirement Title: EMC IT Support Services Contract
Line/Staff Office: NWS, Office of Acquisition and Grants, NCEP / EMC

Relevant Past Performance Experience

- (PPR13) NOAA Grants Online (GOL)
- (PPR4) Department of the Treasury Application Support Services Contract

Requirement Title: Oceanographic and Engineering IT Support Services
Line/Staff Office: NOS, CO-OPS/ISD

Relevant Past Performance Experience

Released Small Business

Requirement Title: WR SharePoint Migration Manager Software
Line/Staff Office: NWS, Western Region Headquarters

Relevant Past Performance Experience

Released Small Business

Requirement Title: Administrative Systems Management Division Support
Line/Staff Office: Office of Chief Information Officer, ISMO/ASD

Relevant Past Performance Experience

Released Small Business

Requirement Title: Tech. & Systems Engineer for Science. Data Stewardship
Line/Staff Office: NESDIS, NGDC

Relevant Past Performance Experience

- (PPR8) NOAA/NMFS Science Information Management and Scientific Research Information Technology
- (PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development
- (PPR7) NOAA/NOS GIS and Web Consulting, Electronic Navigational Chart (ENC) Quality Assurance

Requirement Title: Sunflower Asset Systems Support Services
Line/Staff Office: Chief Administrative Office, Personal Property Management Branch

Relevant Past Performance Experience

- (PPR4) Department of the Treasury Application Support Services Contract
- (PPR10) GSA Consolidated Information Systems – ROCIS III
- (PPR11) General Services Administration, Public Buildings Services
- (PPR12) American Chemical Society – Web Application Development

Requirement Title: OCWWS IT Support
Line/Staff Office: NWS, Office of Climate Water and Weather Services

Relevant Past Performance Experience

Released 8(a) – Waiting for Award

Requirement Title: Specialized Technical Systems Administration (PSD)
Line/Staff Office 1: OAR, Physical Sciences Division
Line/Staff Office 2: OAR, ESRL Global Systems Division

Relevant Past Performance Experience

- (PPR14) NOAA/NWS Sterling Field Support Center
- (PPR5) NOAA/NWS Office of Hydrologic Development IT Infrastructure Support
- (PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development
- (PPR4) Department of the Treasury Application Support Services Contract

Team CyberData's Past Performance References

(PPR1) NOAA/NWS Dissemination Systems Branch and Telecommunication Gateway Support

Team Cyberdata supports multiple mission critical dissemination systems for NWS. As a result of our support to some of these programs, aviation weather data is now being disseminated to more than 95 countries via the International Satellite Communications System (ISCS) and more than 98 percent of Americas can receive emergency all-hazards broadcasts via the NOAA Weather Radio (NWR) All-Hazards Network. Our support for these systems has ranged from the design and installation of a COOP site for the Telecommunications Gateway, to support of installation of VSAT terminals in countries worldwide, to the authorization and accreditation (A&A) of these systems. RCG has supported NWS in performing all aspects of A&A activities from the development of SSPs to the creation and tracking of POA&M.

Team Cyberdata has supported the Dissemination Systems Branch for more than a decade. We provide support for program management, GIS mapping, desktop services, web portals, remote installation and maintenance, telecommunications, database and records management, configuration management, and various other functions. We have been tasked to provide A&A support to multiple dissemination systems, including NOAA Weather Radio, ISCS, NOAA Weather Wire, the Radar Operations Center, and Upper Air. Team Cyberdata dispatched A&A engineers to various locations in the country, such as the Radar Operations Center in Norman, OK, to perform these activities.

Team Cyberdata identified system risks by reviewing system security documentation and conducting vulnerability scans on the systems. This information was then compared to applicable guidance and legislation, including NIST Special Publications, FISMA, DOC's IT Security Program Policy, and FIPS 199. Based on their review, they wrote reports of their findings and made the necessary recommendations.

Team Cyberdata staff conducted A&A and ST&E testing, including assisting with defining system boundaries, creating and updating security documents, performing security control assessments, and documenting security. We reviewed and provided analysis of vulnerability scan to identify vulnerabilities, risks, and security issues.

Team Cyberdata's security services spanned the full developmental life cycle, from system inception to system disposal. Team Cyberdata's use of standardized, repeatable IT service management policies and procedures mitigate service deviation, reduce risk to service delivery, promote efficiencies, and build a robust governance model for increased oversight to support informed decision-making.

They established processes and procedures for incident response, configuration and change management, and have performed penetration testing and vulnerability scanning. Some of their security tasks under this contract include:

- Plan system A&A, collect A&A artifacts, and schedule A&A activities
- Prepare briefings for A&A kick off meetings
- Develop, document, and update SSPs
- Conduct rules of behavior and rules of engagement
- Conduct SSP Workshops to review management, operational, and technical controls
- Organize SSP supporting artifacts and update the NIST 800-53 Rev. 3 Controls Analysis Spreadsheet to map artifacts into applicable security controls
- Create system definition and system boundary scopes
- Perform security categorization, per FIPS 199 and select and review security controls, per NIST

800-53 Rev. 3

- Create and update Incident Response Plans
- Draft AO briefings, and prepare ATO briefings
- Prepare/Review and update security briefings
- Create, review, track, and update the POA&M
- Conduct/Coordinate vulnerability scans and penetration testing
- Draft and update Interconnection Security Agreements, and create MOUs
- Conduct security assessments and update risk assessment report to include applicable risk for findings discovered for the NOAA8223 Security Assessment
- Provide coordination and administration of all security related tasks and C&A for the IT systems under consideration
- Planning configuration management process for all dissemination systems
- Review and research system component inventory to establish baseline security configurations
- Provide administrative support, project management, meeting schedule support, and prepare briefings for meetings
- Document rationale in the FIPS 200 Security Control Baseline Tailoring document
- Create Security Assessment Report, Authorizing Official ATO Briefing, accreditation letter, and configuration baseline matrix.

(PPR2) NOAA Computer Incident Response Team Security Office (CIRT)

Under this contract Team Cyberdata has performed security risk analysis of all major NOAA line office facilities in the Washington, DC area. Team Cyberdata collaborated with the NASA Systems Incident Response Capability (NASIRC), in developing security guidelines and policies that established the NOAA Computer Incident Response Team (N-CIRT) office. Team Cyberdata has been tasked as a responder to computer security incidents involving NOAA infrastructure and systems and is the primary consultant for the development of N-CIRT policies and procedures. Team Cyberdata is responsible for staying informed of regulatory trends, new standards, and new technologies, and reports to NOAA CIO organizations on risk assessments, impact analyses, and recommended security enhancements. Team Cyberdata developed and maintains an interactive security web site and recommends security posture as required in its on-going maintenance of the N-CIRT. Team Cyberdata utilizes the INFOSEC IAM (Assessment Methodology) approach to document to NOAA high, medium, and low level threats, vulnerabilities, risks and appropriate mitigation.

Team Cyberdata is the principle author of the draft NOAA Public Key Infrastructure (PKI) Certificate Policy. Team Cyberdata performed a comprehensive security risk assessment and provided recommendations for securing the NOAA National Virtual Data System, the system is used to provide all NOAA data center information in the public domain. The analysis was the pre-cursor and a primary element in facilitating security "tightening" for this popular and crucial NOAA information dissemination resource.

Team Cyberdata was instrumental in the NOAA PKI Working Group. RCG assisted in writing the NOAA Firewall Implementation Policy and is a member of the NOAA IT Security Architecture Working Group. At the time. In addition Team Cyberdata was called upon to help articulate network security as part of the network restructuring effort of all networks within the Main Commerce Building. The effort entailed writing a department wide security plan, performing a comprehensive security risk assessment and analysis, using the INFOSEC (IAM) methodology to document threats, vulnerabilities and risks. Vulnerability testing is conducted using Harris/NESSUS scanning tool. Team Cyberdata performed

Certification and Accreditation functions and reviews for NOAA and the DOC. Team Cyberdata helped establish the DOC CIRT, setting up Standard Operating Procedures and providing overall guidance. The parameters for the deployed capabilities and documentation included, but are not limited to: vulnerability and regression testing standards; configuration management and oversight standards and policies; incidence response policies and procedures; law enforcement liaison policies; forensics toolkit deployment; and forensics analysis of intrusions policies and procedures.

CIRT staff members designed an interactive Web-based Incident Response System to facilitate functionality of the CIRT. The staff helps support a secure level server, a clear text server, and a data base server. With these and other facilities, the CIRT is able to track incidents in any of the DOC operating units. This interactive web site capability is also used by the NOAA CIRT for incident dissemination and reporting purposes. Team Cyberdata provides training and education of computer security technical support personnel, including awareness training and documentation and supports and conducts training outreach programs.

Extending the scope Team Cyberdata has additionally performed and continues to perform following tasks:

- Implemented INFOSEC Assessment Methodology (IAM) at several Government Sites, provided support for developing IT Security Program compliance metrics
- Drafted PKI Certificate Policies for the NOAA Agencies, advised on IT Security Architecture development
- Provided technical support for the DOC IT Security Task Force and its working groups
- Develop procedures for and Staff for DOC (CIRT) & NOAA (NCIRT)
- Evaluated trust relationships inherent in Web services delivery
- Support & Advise DOC and its operating units on IT security programs (GISRA, FISCAM compliance) and policy (OMB) implementation.
- Conduct or provide assistance to N-CIRT personnel or security technical support (STS) in the investigations of all incidents to include forensics, system recovery, containment and aftermath cleanup.
- Coordinate actions taken by outside entities for responding to NOAA security incidents, i.e., NASA Automated Systems Incident Response Capability (NASIRC) and NOAA's STS.
- Provide user level support and liaison with NOAA's STS.
- Manage up to 10 Internet Security System's (ISS) RealSecure Engines and up to 2 Consoles.
- Support NOAA's TIC initiative.
- Maintain all security patches to the operating system(s).
- Perform vulnerability testing on NOAA networks as necessary to assist NOAA network administrators in locating vulnerabilities in their networks.
- Perform incident forensics to determine the nature of and other pertinent aspects of security violations.
- Advise security staff and system security infrastructure.
- Develop and enhancing a suite of proactive security measures for NOAA.
- Develop configuration management software, capabilities and other security software.
- Promote and advise on appropriate security policy for NOAA systems.
- Oversee vulnerability monitoring to enhance security of NOAA's systems.
- Evaluate, disseminate and implement software tools to minimize system vulnerabilities and improve threat awareness.
- Develop guidelines and procedures for UNIX and NT operating systems**.**
- Develop workshops for system administrators.
- Train the NOAA STS in incident response capability, i.e., recovery/containment of attacks.
- Provide tools and educational training for the N-CIRT web page for the computer security web site.

- Update the current NOAA Computer Security Web site.

(PPR3) Support for the Department of Homeland Security (DHS) programs

For various federal initiatives, Team Cyberdata provides the expertise in the domains of Policy & Strategic Planning, Independent Assessments and COTS Evaluations, Enterprise Architecture (including COTS, Tech Refresh and TO Studies), PMO Support, IT Services Management (Systems & Performance Engineering Support & Documentation).

Under Task Orders 4, 8, 17, and 27, Team Cyberdata led 6 separate Independent Assessments and Trade-Off Studies that led to acquisition of new technologies for Department of Homeland Security (DHS) programs. In one example, Team Cyberdata assessed third-party solutions by conducting International Council of Systems Engineering (INCOSE)-based Trade-Off Studies as part of a large project called Enterprise Service Bus. The hosted solutions examined were rated based on their ability to simplify the integration and flexible reuse of business components within a service-oriented architecture (SOA). The weights assigned considered factors such as price, re-use, TCO, energy footprint, and ability to provide a dependable and scalable infrastructure that connects disparate applications and IT resources, mediates their incompatibilities, and makes them broadly available as services for additional uses. The systems under study took inputs from various sub-systems to be sent to a consolidated portal. Under TO 8, Team Cyberdata conducted Trade-Off Studies for the selection of performance measurement and monitoring tools for enterprise networks. The study focused on hardware, software, and human factors, including the 508 and Human Factors Engineering (HFE).

Under several FA&E and PMO Support Task Orders (TO 4, 8, 12, 15, 16, 17, 21, 22, 27, and 31), Team Cyberdata consistently provided foundational architectural, engineering, and PMO support for the modernization of CBP Systems and Networks. In addition, Team Cyberdata's Systems Engineers, Data Architects, and SMEs provided expertise in systems & COTS integration support, as well as performance engineering, using hardware and software-based tools such as Agilent J6800A, OpNet, Popkin, and Hyperformix to provide optimization methodologies on release-level, as well as enterprise-level eBusiness arcitectures and systems within ACE. Team Cyberdata staff authored the ACE network capacity bandwidth report, sensitivity analysis, and developed the ACE ENCOSE Technical Performance Measurements (TPM) program for Release 4 and 8. Team Cyberdata has also been instrumental in developing enterprise TEAF business requirements mapping using the RTM tools to align requirements of 60+ subsystems to business objectives. In the ACE framework, Team Cyberdata has also conducted detailed Trade-Off studies in the areas of collection & analysis methodologies for real-time analysis of gigabit WAN networks.

Under the *Entry, Summary, Accounts, and Revenue (ESAR)* and *Cargo Targeting and Enforcement (CTE)* programs, Team Cyberdata consultants conducted Independent Analysis of system performance, which included development of D7 Load Runner scripts, including necessary updates on D7 scripts due to new build deployment and also Legacy scripts (D5); ran and verified legacy scripts on SR-SAT; updated D5 Load Runner scripts on D7 baseline on SR-SAT; tested application for functionality and opening a Problem Tracking Report (PTR) on SR-SAT; executed and updated A1/D5 automated tests on string 3; performed regression tests on D8 baseline on T6; and automated R4 test cases and supported PBE to execute D5 tests. They executed Regression test cases on the NEW ACE strings in support of A1, M1 and also migration of the strings to the new location; worked on TMTP scripts using Rational robot for production' wrote / tested / executed SAT business scenarios as per the requirements for M1 SAT (Technical Lead); developed, drafted test case development for the initial 4 threads as planned from

customer for M1 SIT Lead; and worked with the customer on performance requirements gathering, system performance analysis, and diagnosis.

On TASPO-ATS, another task order on ACE, Team Cyberdata's Performance Engineers provided deep-dive database tuning & analysis on numerous platforms including S2TF Oracle Sigma for ATS, D5 Enforcement, and Transaction SAP databases. The team optimized numerous Oracle & DB2 databases for ACE and ATS. Team Cyberdata analyzed and corrected referential integrity problems, business enforcement rules, and invalid data types that were layered into 20 years of databases. Our performance engineers detected and corrected the most expensive SQL statements that impede performance. The team led IPT recommendations for performance improvements on forward-looking architectures.

Team Cyberdata's Certification and Accreditation Teams developed the test methodologies for the *Automated Commercial Environment (ACE)* M1.1 System Integration testing for thread 1. Team Cyberdata's Testers performed in-depth analysis of Use Cases, requirements, and business rules and developed test cases based on business and systems rules mapping. Team Cyberdata testers performed independent in-depth analysis of the test cases and identified anomalies in the M1 subsystems. Team Cyberdata's Independent Validation and Verification Testers identified and created Problem Tracking Reports (PTR) based on their analysis of the results. They prepared the test inspection package for thread 9 and thread 11 US Government representative on the M1 project. Team Cyberdata helped get thread 1 back on track including, reviewing Business Rules and Use Cases, rewriting test cases, re-creating data, and executing newly identified test cases.

While working on M1.1 System Integration testing Team Cyberdata's Independent Software Integration Testers executed capability level 3 test cases in QC for thread 1 as well as created and executed test cases in the quality center for thread 1 capability levels 4 and 5. Team Cyberdata created data for capability level 3, 4, and 5 on P drive for the test team to use for their test cases. Team Cyberdata created data in X-12 as well as CAMIR format for EDI messages. Team Cyberdata also created the related queries for the test cases to run them, made the cases ready for inspection, mapped all the use case business rules to the test cases, and related RSS's to the test cases. Team Cyberdata worked on the string7 UNIX log files to search for Events sent to ATS and ACS.

Team Cyberdata's Integration Testers supported PBE Testers with String 9 T2 issues and trade testing as well as supported D8 Testers with String 9 T6 issues. They worked closely with developers (EIS/ESNM/Middleware/Portal/TXN/DBA) to correct issues found on T6 and performed test case runs for A2.1 Security on String 5. They performed test case runs for A2.1 Security on String 5 and prepared document for String Owner Regression Testing and assisted the ACE Transaction Team Lead and legacy team to get ready for deployment to PROD (PRR). Our consultants used WinRunner to design and implement automated test scripts, various configuration management plans, software quality program plans, metrics specifications and reports, prepare software test documentation, and manage problem/change reports using Polytron Version Control System (PVCS) dimensions. The Team Cyberdata worked with the ACE Program Management office in developing and changing test and automated test procedures that were later used across the project. This effort involved integration of Java Code, SAP, Websphere, MQ Series, DB2 databases and Informatica Power Center.

Team Cyberdata professionals provided Independent Security Oversight And Security Assessments to the *Operation & Maintenance Program Office (O&M)* and Security Team under *Customs and Border Protection Office of Information Technology (CBP OIT)*. They provided security support using IBM Tivoli Products to Security Control Officers (SCO) of CBP and security test support to the e-Customs Partnership Test Manager. They developed security policy and procedures in support of the Government client as well as security engineering support to Enterprise Architecture team and provided training to the Security Control Officers and Field Security Control Officers of CBP. The Team managed day-to-day

security operations of a 700 plus personnel organization in support of information security, security engineering, systems testing and development and program management.

(PPR4) Department of the Treasury Applications Support Services Contract

Team Cyberdata supports the operation, maintenance, and enhancement of 22 applications spanning 5 application portfolios across all Treasury bureaus and offices. The portfolios include applications that track trillions of dollars in international capital flows, manage regulatory compliance review, and support reporting to Congress.

Team Cyberdata has received 9 Task Orders under this multiple-award IDIQ vehicle—none of the other awarded contractors has received even one Task Order.

Technology Mix – The technology mix includes web-based and client/server applications deployed on a variety of platforms including Oracle, Windows 7 and Windows XP, MS SQL Server, and MS Windows Server. Toolsets and technologies include Java, HTTP, XML, VB Studio, Java script, SQL, PL SQL, Adobe LiveCycle for PDF forms, and high-end Kofax scanners.

Accomplishments – Team Cyberdata accomplishments include:

- Transitioned entire suite of 22 applications from incumbent O&M contractor in 45 days, including complete application inventory, documentation of application business processes, gap analysis, and development of Transition Plan and final Transition Report.
- Restructured the O&M support team to eliminate stovepipe staffing model and replace with matrixed staffing model to ensure more complete coverage and depth.
- Established service level agreements for O&M team and for other contractor support to the O&M team, including infrastructure contractor and outsourced hosting contractor.
- Received option exercises, additional tasking, and multiple new systems added to O&M contract as a result of strong performance during transition and beyond.

Business and Technical Analysis – Team Cyberdata plans, designs, and implements new functionality for Treasury applications as required by business owners. We interview SMEs to gather requirements, and we assess the business and functionality needs in the context of the existing technology platform, new technology alternatives, network and data requirements, and performance requirements. Team Cyberdata creates business process flows and summaries of business and functional requirements, and we prepare budgets, plans, and schedules, with a WBS and formal project plan. Our proposed solutions include alternatives where feasible and solutions address the business needs within the technology and budgetary constraints. We propose process or technology improvements where possible, and we consider the long-term budgetary and security impacts. We develop detailed requirements documents with traceability throughout the project life cycle, and we review requirements with users and business owners to validate their accuracy and completeness.

Operations and Maintenance – Team Cyberdata performs operations and maintenance for all 22 supported applications. For example, Team Cyberdata operates, maintains, and enhances the Document Capture Pilot (DCP) system and the Electronic Wire Transfer Licenses (EWTL) system for the Office of Foreign Asset Control (OFAC). These systems import paper-based license application forms for Electronic Wire Transfers, Cuba travel, and other OFAC programs. Team Cyberdata maintains, upgrades, and enhances the OASIS system, a web-based tracking and workflow system used to process the license applications captured via imaging and document capture. OASIS produce licenses, which are issued to the public, and annually tracks about 15,000 pieces of correspondence, 5,000 licensing cases, 500 enforcement cases, and 300 civil penalty cases. The system tracks the status of license cases and supports the processing of the applications by various staff within the OFAC office. For these and other

systems, Team Cyberdata documents and performs SOPs related to system support and administration, maintains data loading components, monitors and tunes application and query performance, runs diagnostic programs as needed to troubleshoot problems, and maintains all custom code and COTS software under formal configuration control and deploys patches and upgrades in coordination with the Configuration Control Board

After-Hours and Weekend Support – Team Cyberdata provides on-call after-hours and weekend support for all applications. We prepare a coverage matrix identifying the designated staff and escalation points, and we respond to phone and email requests as well as to automated alerts produced by system monitoring functions, and we work with the centralized Help Desk to ensure timely response for all applications depending on the criticality of the application and the issue.

Document Capture and Imaging – Team Cyberdata operates, maintains, and enhances the Document Capture Pilot (DCP) system and the Electronic Wire Transfer Licenses (EWTL) system for the Office of Foreign Asset Control (OFAC). These systems import paper-based license application forms for Electronic Wire Transfers, Cuba travel, and other OFAC programs. The document management system is composed of Kofax scanners, Adobe LiveCycle for PDF forms, O2 Solutions PDF4NET, Oracle 11g DBMS, and Kofax Ascent Capture.

The DCP and EWTL systems convert paper forms to images which are then OCR'd using PDF4NET and Kofax Ascent Capture, and then imported into the Oracle database. The database holds machine-readable information for all fields submitted by the user except the signature, which is captured in the PDF scan of the paper form, and which becomes the record copy of the form.

Team Cyberdata operates and maintains the image content subsystem for DCP, which stores all user-submitted forms as PDF image files in the Oracle database, and associates each image – the record copy – with the corresponding database record created when the user was online, containing the user's submitted input in machine-readable format. Correspondence related to license applications is also scanned and imported into the database, and associated with the user's record.

Team Cyberdata installs, maintains, configures, and trains users on the operation of the Kofax scanners, which capture document images and store them to the Oracle database. The Treasury systems provide the remote, web-based user with the ability to fill and print PDF forms and mail them to Treasury for processing. The web application applies a 2-D barcode to each page that contains all information input by the user into the form for that page. The scanning function reads the barcode on each page and populates the Oracle database with the user's input for the applicable fields on the page. Incoming mail is scanned and metadata entered at the rate of dozens or hundreds of pieces a day. Approximately .5 GB per day is added to the database.

Data Management and Analysis – Team Cyberdata analyzes data requirements to determine the optimal technology and implementation strategy for enhancements. We assess data standards and design data migration and data import solutions to ensure compliance with data formats. We design, manage, and perform the data extract, transform, and load (ETL) operations on a predetermined cycle (typically daily and monthly); and we implement automated loading processes where possible.

Team Cyberdata performs data modeling, database design, performance monitoring, database tuning, stored procedures programming, and SQL-based data queries across a variety of DBMSs including Oracle and MS SQL Server. This service is provided to all Treasury ASSC applications as needed.

Service Desk – Team Cyberdata operates a level 2/3 Help Desk for the Department of the Treasury. We support five application portfolios comprising 22 applications, many of which are enterprise-wide and have high visibility including at the Secretary level. Our Help Desk has standard support hours for onsite personnel, supplemented by 24x7 availability in response to critical system issues. Our team of 18 onsite technical staff are accessed as needed via documented escalation paths.

Testing and Quality Assurance – In support of the deployment of application enhancements and COTS software upgrades and patches, Team Cyberdata designs, develops, and executes test scripts and test plans to support performance, unit, system, and operational testing. We coordinate user acceptance testing and review and validate test results, as well as prepare test reports. We monitor and ensure compliance with application performance against established SLAs.

Technical Writing – For each new application release, Team Cyberdata prepares formal documentation including deployment plans and updates to System Administration manuals and User Guides. We support the development of SOPs and disaster recovery plans by interviewing SMEs and business owners and attending meetings with technical and business managers, often documenting the meeting minutes. We prepare technology alternative and strategy white papers for OCIO consideration and use in agency IT strategic plans.

(PPR5) NOAA/NWS Office of Hydrologic Development IT Infrastructure Support

Team Cyberdata provides Infrastructures support services to the National Weather Service Office (NWS) of Hydrologic Development (OHD). Our highly talented team of Systems Administrators support a vary diverse environment that must be managed for high availability and utility in order to provide a stable computing environment for the development and testing of software, science and information systems. This environment is used by over 90 developers, scientist and test engineers developing products and services for the National Weather Service and its customers. Our team provides day-to-day support, maintenance, monitoring, and troubleshooting of the OHD Development Environment-Information Technology (DEIT) computing environment, including support for the Linux and Windows systems, LAN servers, websites, web pages, storage and backup systems.

Description of Work

Team Cyberdata runs the IT Systems Group (ITSG) for OHD which is composed of a Service Desk based environment functioning on a multi-level tiered approach. Tier 1 Systems Administrators handle the initial contact, assess the problem and either handle the incident or escalate the ticket to the next available SA, or Tier 2 /3 technicians, to resolve the problem. We handle over 130 devices, of which 75 are servers and 15 are switches/routers, including Virtual Machine configurations, RAID storage, network IT security concerns, and software patch management policies and procedures. RedHat Enterprise, Legato and Windows are currently supported. Our team implements and enforces new policies and procedures and supports the deployment of new hardware devices such as servers, printers, and network devices. Recently the ITSG team configured 2 new AWIPS machines where they were to receive radar data to be used by multiple development teams. To improve our support services, we improved the ticket tracking process by converting the current system from Bugzilla to Mantis. Users have been trained in the use of the new system, and can interact with it via email or web.

Team Cyberdata provides support to the OHD ISSO by routinely implementing security controls. As the result of the systems A&A certification process, our team installed McAfee Linuxshield virus scanning software on our hosts to satisfy a POA&M. The installation proved to be a challenge in that it often crashed our machines. Team Cyberdata was able to determine what was causing the crashes and disable that feature. The team subsequently wrote scripts that updated the definition files and ran routine scans on the machine.

Team Cyberdata provides Network Engineering services in support of the OHD system. Our team supports the OHD DMZ by providing network design and implementation services in support of the OHD subnet. The ITSG team works with NOAA's Network Operations Center to configure firewalls and to resolve connection problems. Significant changes have been made to the OHD network that have been in

place for years, such as the virtual machine sharing IP space with the HADS system have been moved to their own small subnet. This not only improved the operational support for HADS, but also improved its security.

Team Cyberdata's ITSG group provides comprehensive monitoring of its server environment. To improve this capability we replaced the old unstable Pentium II log monitor and implemented a new, more in-depth, VM monitoring package called Logwatch. This monitoring tool aids in the identification of problems and their related causes.

The ITSG team also supports the storage environment for the OHD environment. Under CyberData's tenure, the OHD environment suffered a critical, unreported outage of their primary storage system. Working after-hours, our team recovered the storage environment and data with minimal downtime and no loss of data. Having listen to the vendor, OHD would have lost all of its data (over 12T) and their staff of over 90 developers and scientist would have been idle for at least two weeks. Our team has also been able to improve the instability of the storage system and lower the risk of sudden catastrophic data loss.

Team Cyberdata also provides consulting services to OHD for the evaluation and recommendation of new tools and technologies. Our ITSG team worked with OHD to select virtualization software, backup tools and processes, and storage devices. ITSG, working without documentation or institutional knowledge, identified and documented a public-facing ftp server and created an account for a remote user to upload flood data. We completed the CPSBN hardware refresh documenting the process and ensuring a full supportability. This implementation freed up hardware for a new firewall as part of the splitting of the HADs boxes away from the Virtual systems. Using the monitoring system, ITSG discovered that the HP/Lefthand storage systems had a large number of unreported errors (and 9 bad drives). Replacements were installed and data integrity was ensured after hours and over the weekend. Urgent storage needs were met with the new storage system, although testing has shown that it is not a solid long-term solution. Team Cyberdata provided storage quotes for faster, more reliable Isolon units from govconnect.

(PPR6) NOAA/NWS Office of Hydrologic Development Scientific Application Development

Team Cyberdata provides IT support services in support of the NWS Office of Hydraulic Development (OHD). OHD's mission is to develop and deliver valued science, software and information for river and stream forecasts to save lives and enhance America's economy. We assist in this initiative by transferring scientific advances in the areas of hydrology, hydrometeorology, and hydraulics from the research arena into operational software applications.

Transferring scientific advances into operational software involves analyzing a validated prototype application developed by the OHD Hydrologic Science and Modeling Branch (HSMB) and other partners and integrating it within the NWS operational environment provided by the AWIPS Program at Weather Forecast Offices (WFOs) and River Forecast Centers (RFCs). It also involves developing and enhancing scientific applications for the OHD Community Hydrologic Prediction System (CHPS) which is being fielded on AWIPS systems at RFCs. Team Cyberdata supports these efforts by employing a variety of software engineering tools and techniques to accomplish this task.

Team Cyberdata supports NOAA Community Hydrologic Prediction System (CHPS). This system enables NOAA's water research and development enterprise and operational service delivery infrastructure to be integrated and leveraged with other federal water agency activities, academia, and the private sector. Our team provides systems engineering support through systems analysis, design, development, testing, configuration and deployment. With an in-depth understanding of Hydrologic principles, we are able to integrate complex scientific algorithms in support of these NWS requirements.

(PPR7) NOAA/NOS GIS and Web Consulting, Electronic Navigational Chart (ENC)

Team CyberData provides support for the Marine Chart Division, Coast Survey Development Laboratory, and the Office of Coast Survey on the NCS-II Project. Activities include: 1) Geographic Information System and web consulting, etc.; 2) Consulting services and studies; 3) Management support activities; 4) Electronic Navigational Chart (ENC) quality assurance, etc.; 5) Customer support for Ofc of Coast Survey Inquiry and Discrepancy; 6) ENC data collection, quality and harmonization analysis and services, etc.

Description of Work

Team CyberData provides project management and technical activities in support of the NCSII Transition Project. As the electronic distribution of NOAA chart products to commercial and consumers continues to increase in importance, Team CyberData supports NOAA in the accuracy of chart products and the processing of source and distribution of chart products. Team CyberData provides a unique mix of technical, marketing, chart user, and chart distributor perspectives to enhance the MCD website and refine MCD's web applications to support customers. We use defined standards and processes that include formal documentation and code reviews for software development. Team CyberData is thoroughly versed in International and United States electronic chart standards and formats. Team Cyberdata understands the NOAA's RNC and ENC distribution network. Team Cyberdata provides critical support to NOAA for the accuracy and quality of navigational charts. Team CyberData has been instrumental in the implementation of ISO 9000 quality standards within the Office of Coast Survey in all aspects of electronic charts. Team CyberData has completed the following activities under this task:

Activity A - GIS and Web Consulting Services

a. OCS System Development Lifecycle, OCS Portfolio Management, and Project Execution: Team Cyberdata has led the effort to develop a System Development Lifecycle (SDLC) for the Office of Coast Survey. This effort included design of a custom lifecycle, authoring of associated project artifacts and templates, and benchmarking the SDLC against other lifecycles. We assisted in the design and implementation of the Project Review Board and authored the SDLC Policy document. The project was completed on-time and in ten months.

b. Microsoft SharePoint Support: Team CyberData has developed mission critical SharePoint sites for OCS and MCD. Major sites built to date include: the Quality Management System, the QMS Manual and the Project Center. Substantial analysis, design and development have been completed on other SharePoint sites within MCD. These include: MCD's NCSII Site, MCD's Nautical Chart Manual Site and specific Project Center Project sites, for example, The Bathy Gridded Database Site. Having all documentation, and project related information in one place, OCS and MCD can ensure that the correct information gets to the right individual at the time needed.

c. Publish documents and GIS information on the web: Over the past year MCD has taken more responsibility for the web distribution of its products. A new website has been developed to replace the CARIS Chartserver website. Team Cyberdata participated in development by writing software to help with the packaging of ENC datasets. We developed a graphical user interface to the system based on the Google Map service. This interface provides the public with a visual means of finding and selecting OCS navigation products. In addition, Team Cyberdata created a software development process. The benefits of the new software development process has been lower risk of software failure, a higher match between the end result and initial goals, higher quality software, increased transparency, more accurate status updates, and easier transition during staff turnover.

d. NCSII: With the decision to move to NCSII, Team Cyberdata has been instrumental in bringing that system on-line, from the modifications to the DREG system to the development of the Converter. The Converter is the second part of a two part process which enables the communications between NCSI and NCSII, this two part processes is called the Extractor/Converter. Team Cyberdata participated in the design of the Extractor as well as the design and development of the Converter. Team CyberData is also

working on components which will support NCSII with the eventual goal of moving to a fully integrated NCSII system which will include the Esri Charting component.

Activity B - Consulting Services and Studies

Lynker has provided support to the Office of Coast Survey in the implementation of a quality management system (QMS). The QMS has been implemented to ISO 9001:2000 Standards. Team Cyberdata has developed the QMS Manual, Standard Operating Procedures, and Work Instructions for OCS. In addition, Team Cyberdata developed and provided extensive QMS training for OCS executives and staff.

In addition, Team CyberData was responsible for and has created a QMS SharePoint site for OCS. The QMS site houses the three major components of OCS' QMS. Second, a separate "OCS Records Center" site has been created to manage OCS' Records in accordance to the QMS' "Control of Records" standard. Third, the QMS Manual, a required component of the Quality Management System was built using SharePoint WIKI technology.

Activity C – Management Support Activities

Team Cyberdata supports NOAA in the management of NOAA's RNC and ENC distribution network. These support activities are an important link from NOAA to distributors and, ultimately, ENC or RNC chart users. We use our onsite presence to ensure effective operation of these programs. Our team evaluates all RNC and ENC requests using the Code of Federal Regulations on how to become a certified distributor for those products.

Activity D - Electronic Navigational Chart (ENC) Quality Assurance

Team CyberData provides for the composure, Quality Assurance and publishing of critical updates in the BSB format for new editions and update patches for the suite of Nautical charts according to established process workflow. Updates are provided twice weekly in the BSB format and other formats as well.

We utilize the NOAA BSB process in use at Marine Chart Division. Discrepancies found are sent back to the production team for correction. As new systems come online, and the BSB process evolves, our team continues to analyze the BSB process looking for opportunities for it to be streamlined.

Activity E - Customer Support for Office of Coast Survey Inquiry and Discrepancy

Team CyberData provides customer communication support as a tool to enhance customer satisfaction and collect valuable information to improve products and their delivery. The Office of Coast Survey Inquiry and Discrepancy (IDMS) System is an important channel to chart users. Team CyberData provides help desk support allowing mariners to call for chart assistance.

Activity F - ENC Data Collection, Quality and Harmonization Analysis and services

Team CyberData produces new ENC data for NOAA and for providing data quality and harmonization analysis services. For ENC collection, our team receives source data (i.e. the raster chart) and chart limits from NOAA, which is then digitized, encoded, and validated to produce an S-57 ENC. The deliverable is then submitted to NOAA as an exchange set. We provide support in meeting and verifying higher levels of quality in NOAA products for use on maritime vessels. We perform independent ECDIS and ECS testing of ENCs as required. We support an additional layer of quality control for the ENCs by having these charts evaluated using a variety of different navigation systems (ECDIS, and ECS) to ensure that the mariner will not encounter problems with this data. Lynker supports this additional level of quality assurance using ECDIS and ECS tools and IHO standards. Lynker also developed and provided S-57 training for MCD.

(PPR8) NOAA/NMFS Science Information Management and Scientific Research Information Technology

Team Cyberdata supports the Department of Commerce, National Oceanic and Atmospheric Administration (NOAA), National Marine Fisheries Service (NMFS), Office of Science and Technology (ST) to ensure the quality and integrity of its scientific activity, including the quality and credibility for scientific information. Our customer is the primary interface between the NMFS scientific activity and

NOAA, other agencies, and international organizations. It has oversight of NMFS scientific research and technology development activities, including marine biology, ecology, economic and social sciences, oceanography, management of scientific information, engineering, and other disciplines used to fulfill its mandate to conserve and manage our nation's living marine resources through its divisions.

Team Cyberdata supports the Science Information Division in the maintenance an operation of its applications, database servers and file servers. In supporting the OST mission, Team Cyberdata provides expertise, professional services and tools in support of the . Team Cyberdata also provides expertise and professional services with program and project management support in the NMFS Office of Science and Technology.

Our services include System Architecture development expertise, Systems Administration, Oracle Database Administration, Application Development, Technical Project Coordination and Management, System Analysis and Technical Writing and System Testing support.

(PPR9) Department of Commerce Information Technology (IT) Helpdesk Support Services

Team Cyberdata provides support to the Office of the Chief Information Officer (OCIO) office for IT support and administration through the implementation of a full-service IT Help Desk. Cyberdata operates the IT Customer Service Center (ITCSC) to support customer requirements relating to hardware, software, and systems used to collect, process, store, transmit, and disseminate data and information. This includes personal computers (desktops and laptops); hand-held computing devices; printers, copiers, scanners, and other peripheral IT equipment. Requirements may also involve the planning and delivery of customer support services, including but not limited to information gathering, installation and configuration of hardware and software, and assistance in response to customer service requests and troubleshooting.
To sustain the operational capacity and quality of services rendered within the current environment in support of the OCIO and its customers Team Cyberdata provides the following services.

- Problem Management
- Incident Management
- Configuration Management
- Change Management
- Release Management
- Service Desk Functions
- Service Level Management
- Availability Management
- Capacity Management

(PPR10) GSA Consolidated Information System—ROCIS III

In support of the Regulatory Information Service Center (RISC) and OMB Office of Information and Regulatory Affairs (OIRA), CyberData developed a White House portal for Presidential Executive Order review and rulemaking. It provides an interface between RISC/OIRA and all 60 Federal agencies for collaboration in data exchange, regulations, and reporting.

ROCIS is also used to publish the semiannual "Unified Agenda of Federal Regulatory and Deregulatory Actions and Regulatory Plan". The ROCIS historical data (early 1980s and forward) provides a rich store of information for data mining and sharing.

The ROCIS architecture consists of a mix of application software, Oracle/WebLogic Portal, COTS document management software (Documentum), and an RDBMS developed using the Java 2 Enterprise Edition (J2EE) Frame Work 2 platform as well as the J2EE software organization and conventions. Through disciplined adherence to these conventions, CyberData helped ensure that the ROCIS system was platform independent, able to take advantage of future technology enhancements, and easily supportable by virtue of our large and established base of industry expertise in this technology.

Transition Support
The CyberData team began work after problems developed with a prior incumbent's attempt to stand up a production ROCIS system. The level of manual intervention required to operate the system and the lack of collaboration with agencies were of great concern. In parallel with CyberData ramp-up activity, workarounds were implemented to stabilize the system. CyberData then proposed and implemented a follow-on redesign of ROCIS with a focus on best-practice portal application and database design, automation of data load and reporting, data quality management, and implementation of expert recommendations on architecture and process standardization

Summary
Following the successful launch of the redesigned ROCIS system, the project team was invited to the Indian Treaty Room at the White House for a formal commendation by Dr. Don Arbuckle, the Deputy Administrator of OIRA..

Virginia Government Business One-Stop System (http://bos.virginia.gov)
CyberData has also worked with VDBA to accomplish a major redesign and rewrite of the BOS-REG (Business One-Stop Portal) system. BOS-REG is a web portal and business registration system that is used by the business community to learn about doing business in Virginia and to submit new registration. BOS-REG the ongoing needs of established businesses regarding licensing and other forms, and is integrated with several external systems, including Federal and State agencies. CyberData utilized its extensive technical experience to redesign and rewrite the BOS-REG system, enabling the system to be integrated with newer technologies and fully compatible with mobile browsers.

Technologies Used:
Oracle AS 11g/WebLogic, SSO, OID, Java/J2EE, JavaScript, Struts, XML/Web Services, SOAP, UML/Rational Suite, JDeveloper, Crystal Reports, Oracle Reports, Oracle RDBMS 11g, Oracle Data Warehouse Builder, Erwin, Sun Solaris, WinRunner, LoadRunner, (EMV Tool) Dekker Trackker , MS Project, MicroComp, Documentum

(PPR11) General Services Administration (GSA), Public Buildings Service (PBS)

Team CyberData architected, designed, is iteratively building, and maintains the PBS BI Framework. The PBS BI Framework is built on the Oracle Business Intelligence Suite Enterprise Edition (OBIEE), which is a comprehensive enterprise BI solution that delivers a full range of analysis and reporting capabilities. Featuring a unified, highly scalable, modern architecture, PBS BI Framework provides intelligence and analytics using data drawn from enterprise sources and applications—empowering the largest Government real property management communities with complete and relevant insight into the business. The PBS BI Framework has:

- Established a superior PBS-wide Data and Information management architecture.
- Provided a foundation that can scale economically over time to handle virtually limitless data growth and user demands.

- Enabled access to information through a broad range of interfaces and modes such as dashboards, alerts, and reports.
- Integrated seamlessly into business processes and workflows.
- Provided relevant and accurate information to all users at the time it is needed.
- Facilitated access to timely, accurate data.

Accomplishments – Team CyberData has accomplished the following under this project:

- Recommended and implemented data warehousing hardware/software architecture featuring Oracle RDBMS, OBIEE, Oracle Portal, and Sun Solaris.
- Created a fully functional business-line focused Application Showcase using OBIEE, highlighting cutting edge reporting/mining features for PBS data.
- Assisted in preparing documentation required for Interim and Full Authority to Operate (IATO/ATO), as well as system Certification & Accreditation (C&A) and FISMA compliance.
- Integrated the BI Framework foundation platform and applications such as BI-InfoWizard into the PBS Portal/SSO/eCommon (SOA) architecture, including user access to dashboards, reports, and other information views.
- Successfully rolled out Business Intelligence functionality to selected PBS Line Offices, including training.

Testing & Configuration Management Support – Team CyberData performs unit, system, and regression testing on all developed software. Team CyberData develops the test plans and scripts, executes the tests, coordinates deliveries back into production and manages the configuration management process for code promotion. All code and documentation is maintained under formal CM control.

Application Maintenance Support – Team CyberData provides systems administration, software upgrades, enhancements development, troubleshooting, and tier 2/3 help desk support for the Data Warehouse and BI web-based applications and feeder systems interfaces. This includes Requirements Definition, High Level and Detailed Designs, proof-of-concept prototyping, unit testing, and user and system documentation. Team CyberData designs and builds dashboards, reports, and ad-hoc reports as well as user-defined reporting capabilities.

Oracle Database and Systems Administration/Operation and Application Server Administration – Team CyberData provides operational support and database administration for the Oracle Data Warehouse, Oracle Application Server, Oracle Business Intelligence Enterprise Edition, and application modules. Team CyberData plans and performs Oracle upgrades/migrations, patches, and database monitoring and tuning. Team CyberData implemented Oracle security features and auditing capabilities, role-based access control, and user authentication via OID.

Application Development

Data Warehouse – Team CyberData designed and maintains a relational Enterprise Data Warehouse (EDW) that comprises data from multiple national PBS applications. The data is taken from the source system, then data mapping, data profiling, data cleansing, and data filtering is done before it is stored in the EDW.

Business Intelligence Reporting – Team CyberData designed and maintains Business Intelligence reporting that structures data to enable smarter business reporting. The data is taken from the Enterprise Data Warehouse and organized into dimensional models to facilitate ad-hoc and trend reporting.

Technical Architecture & Systems Integrity – Team CyberData architected and designed the hardware and software platform, and performs capacity planning, supports disaster recovery planning and risk assessments, and supports security and section 508 compliance reviews. Team CyberData participates on

PBS governance bodies to help ensure a consistent and effective PBS architecture that aligns with PBS IT strategy and standards.

SSO Integration – To accomplish Single Sign-On (SSO) integration, Team CyberData focused on the PBS Portal SSO implementation, including Oracle Internet Directory (OID). OID is a central repository and processing point for user identification, authentication, authorization, security policy, access control, and session management. In addition, the PBS Portal implements the User Identity Management System (UIMS), which is a Web application that provides PBS Portal account/password management, access to Single Sign-On applications, and audit reporting that includes monitoring of user/role privileges.

Team CyberData, working closely with the PBS Portal Team, created BI users and roles in OID via UIMS. BI and SSO integration is accomplished via a direct interface to OID—a BI user is registered in the LDAP server, and his login and logoff URLs are defined along with LDAP integration parameters. SSO between the OBIEE Repository and the Web Catalog is internal to OBIEE and done through impersonation; SSO is implemented using OAS native integration with OID.

Team CyberData resolved issues that impacted the SSO integration. The issues arose from the fact that user roles and role assignments in UIMS can be out of sync with their counterparts in OID, and different procedures exist for user creation and account management in OBIEE Repository, OBIEE Analytics, and Oracle BI Publisher.

SOA Integration – Team CyberData's design and implementation of the PBS BI Framework took into account the integration requirements of eCommon, the PBS Service-Oriented Architecture (SOA) environment. The system design took advantage of the Oracle architecture to answer the functional requirements of the PBS BI Framework, while maximizing the system scalability, flexibility, and interoperability. By working closely with the eCommon technical team, the Team CyberData BI Framework team ensured that the system design aligns with and complements the new eCommon architecture. The two teams worked together to ensure that the BI Framework design can take advantage of services deployed on the eCommon Framework, and that appropriate services developed for BI Framework are registered on the eCommon Framework.

Problems Encountered and Corrective Actions – During a migration/consolidation project, Team CyberData found the same data was stored twice in two different systems. Even more challenging, the data was inconsistent when the two sources were compared, and the data was used to establish a dimension in the BI data warehouse. Making a mistake in designing the dimension was likely to have costly ripple effects. Team CyberData discussed the differences between the two sources with Subject Matter Experts to assess data quality within each data set. Team CyberData then selected the best combination of data from the two source systems to create the dimension. Finally, Team CyberData designed both sets of Business Intelligence reporting for the two different source systems to use the same dimension. This ensured consistent reporting across the organization and enabled comparison of the results across the two systems. It also enabled effective analysis across the data warehouse as a whole.

Program Management – Team CyberData manages all technical staff and coordinates with other vendors to troubleshoot problems and coordinate service windows. Team CyberData participates in GSA governance bodies to help ensure a consistent and effective PBS architecture that aligns with PBS IT strategy and standards, and prepares briefings, presentations, and technical recommendations.

Summary – All deliverables and contract services performed under this contract have met or exceeded client expectations. Team CyberData has delivered all tasks contract-to-date on time and within budget, and has a 100% acceptance record for all invoices and deliverables under this contract.

(PPR12) American Chemical Society Web Application Support

Team CyberData worked with the ACS project team, stakeholders, and user community to design, develop, deploy, and enhance the ACS Web portal, which provides Single Sign-On access to an integrated suite of Web-based applications and information. The Portal supports 5,000 internal (Intranet) users, and 10,000 external (Internet) users, for a total of 15,000 users. Team CyberData performed an architectural analysis and provided recommendations to ACS for the to-be hardware and software architecture, which were accepted and implemented. Team CyberData developed the Portal using an

Oracle/Sun-based platform, and provided all system administration and development services to develop, tune, test, and deploy the Portal to production.

Team CyberData implemented a standardized process and infrastructure for designing, developing, deploying, and accessing Web functionality throughout the entire ACS organization. Team CyberData designed the custom portal look and feel, and defined the types of portals to determine the type of personalization for each class of user, and developed a strategy for user access to applications. We implemented a federated portal that reflects a plug and play Service Oriented Architecture (SOA). The architecture includes Web Services for Remote Portlets (WSRP), which allows portlets to be decoupled from portals.

Team CyberData developed user interface graphics, cascading style sheets, JavaScript functions, skeleton JSP files, layouts, and portal, portlet (including pre-built portlets from Portlet Library), book, and page files. We customized WSRP communication and configured WSRP producer capabilities. Team CyberData created property sets with default values, campaigns, placeholders, content selectors, and developed JSPs and Page Flows that implement campaigns, placeholders, and content selectors. We configured declarative security in deployment descriptors to control access to EJBs, URLs, and file-based resources (such as JSPs); created property sets to support expression-based visitor entitlement, and delegated administration roles. We also developed subscription mashups, data mashups, and ACS enterprise mashups.

Team CyberData developed and deployed Personalization features, such as Campaigns, Content Selectors, Placeholders, User Segments, and Rule Sets. Developers can also create rules for Personalization and events for Behavior Tracking.

Team CyberData integrated the portal functionality with content management functionality for the Business Lines, using a collaborative approach for development and ongoing maintenance/enhancement. CyberData provided:

- Categorization (automatic classification and categorizing), defining the terms repository, type, property, node, and library services.
- Faceted Taxonomy, Business Activity Taxonomy, Hierarchy, Business Activity Taxonomy.

Team CyberData's implementation provides social network functionality (ACS network communities), private and public groups, surveys, and feedback, and provides a dedicated, secure, self-managed place for work groups, partners, or other groups to collaborate and share information.

Team CyberData set up and administers security, developed a security strategy and implemented it using portal security policies. We customized the cache settings for the Entitlements Engine, secured the Portal Administration Console, Database Communications, WSRP Applications, UUP Data, and Implemented Authentication Programmatically.

Team CyberData designed the entire web navigation environment, designed web graphics including scientific illustrations for ACS, and produced electronic newsletters.

Team CyberData developed and supports the ACS enterprise-wide messaging backbone based on Java Message Service.

Team CyberData is providing systems development and maintenance for all ACS divisions and customers. Team CyberData designed and developed the Enterprise Shared Services Platform to interface internal and external applications with the Association Management System. The platform was designed

based on SOA best practices with well-defined reusable interfaces deployed on a Mule Enterprise Service Bus (ESB). The ESB/SOA project was implemented on both J2EE and .NET platforms. The open source ESB product Mule, as well as XFire, JAXB, SOAP and WS-Security, were used. SoapUI was chosen as a tool for functionality and performance testing.

The first application deployed on the SOA platform interfaced a WebLogic Portal with Avectra netForum and handled over 100,000 users. The second application deployed was the National Conference Registration application.

Team CyberData staff worked with the ACS to design and develop a financial Business Intelligence framework, including:

- Business case assessment – determine the business need, assess the operational sources and procedures, determine the BI application objectives, perform a cost-benefit analysis, perform a risk assessment
- Enterprise infrastructure evaluation, technical infrastructure evaluation and non- technical infrastructure evaluation
- Software and hardware architecture recommendation
- Project planning
- Project requirements definition and requirements management
- Review existing data, and data analysis
- Extract/transform/load design and data warehouse and data mart implementation
- Business intelligence application development
- Data Store operations and maintenance support
- Business Intelligence application enhancements
- Single Sign On and Security implementation
- User Training

Team CyberData's BI implementation for ACS includes dashboards, easy-to-use ad hoc queries, intelligent interaction capabilities, enterprise reporting, financial reporting, OLAP analysis, and data mining. The BI suite is available to users via the ACS Portal and includes the Team CyberData-built Web-based J2EE applications, which support sophisticated calculation and aggregation infrastructure. The BI dashboard is a full Web-based self-service alert creation and subscription portal, which is actionable and dynamically personalized based on the individual's role and identity. Report formats are designed using Microsoft Word and Excel, HTML, and Adobe Acrobat and can be sent to users via email, dashboards, and mobile devices. Team CyberData continuously enhances and supports the ACS' Business Intelligence and data warehouse/data mart development processes.

All development is performed in accordance with ACS enterprise standards for application look and feel, content, and architecture. Team CyberData and ACS work together to prioritize the scope and rollout of tasks and resources. Using this approach, we have successfully built the first data mart for ACS' membership management business line. Our team of professionals works closely with the ACS members to meet aggressive deadlines as we provide full SDLC support, including application enhancements.

Team CyberData architected, designed, developed, tested, and implemented a Single Sign-On environment for ACS, including identity management and access management capabilities. The SSO environment was implemented using existing Microsoft Active Directory and LDAP functionality. The SSO environment and identity and access management frameworks conformed to ACS enterprise architecture standards.

Team CyberData provides an enterprise-wide Identity Management system to support the heterogeneous IT environments prevalent in the ACS organization. Team CyberData implemented a standards-based identity management solution that:

- Supports all major ACS infrastructure IT systems, including the ACS Portal, application servers, enterprise applications, directories, and operating systems
- Enables cost reduction, increased security, improved user productivity and regulatory compliance.
- Provides SSO for ACS users and business partners, including integration with SAP infrastructure, across organizational borders and uses advanced technologies such as federated identity management.

Team CyberData's implementation manages user access not only for applications, but also to collaboration environments such as portals and portlets. To provide secure and auditable user access across these heterogeneous infrastructures, Team CyberData manages user accounts and privileges, authorizes or blocks user access according to user roles, and protects resources via strong authentication methods such as security tokens. Team CyberData designed and developed a centralized policy and identity administration service across ACS enterprise platforms from Microsoft, as well as custom-built applications. It enables organizations to meet compliance and governance requirements while keeping costs under control.

Team CyberData designed and developed an Access Management system to control all access requests and, based on centrally-stored and managed policies, challenge the end user for authentication according to the required security level. Microsoft Active Directory domain logon via Kerberos tickets and impersonation is also supported, such that the Access Management system can trust a session initiated in the user's Windows desktop. Delegated administrators can easily maintain ACS enterprise security policies by making use of pre-configured authentication types such as form-based login and SecureID tokens to protect the resources at the appropriate level. Based on access security policies, tokens, and cookies, the system provides a seamless SSO user experience.

Team CyberData's Access Management system also provides a central policy store for authorization of users to applications, protecting HTTP, J2EE, and other resource types. The authorization policies are enforced by standard agents as well as modules integrated with application servers. Team CyberData's applications use a standard interface to request information about authorization in familiar environments, eliminating the need for proprietary custom policy enforcement code. These generic authorization policies are centrally stored and easily configured through the Access Manager administration Web interface.

Team CyberData provides master audit rules for identity administration, policy management, and access events. The auditable events include authentication success/failure and authorization success/failure. Each audit trail entry can be configured to capture various details about the event, such as user profile information, the network where the request originated, the Web server involved, the authentication level granted, etc. In addition to master audit rules, individual audit rules can be enforced to capture additional information as required by each protected application. Thus, all roles, permissions, and access events can be audited for applications and portals and for all other applications managed by the Identity Management solution. Audit trail information is typically sent to a central audit database.

Team CyberData's Identity and Access Management system is architected for SOA environments, allowing applications to utilize shared services via standards-based interfaces so that additional applications can be deployed as loosely coupled reusable security services.

Our work for ACS demonstrates our experience and success in managing an enterprise SSO environment and associated identity and access management infrastructure.

Team CyberData performed all services requested at or above customer expectations, and made all deliverables on time. Team CyberData has a 100% acceptance record for all deliverables and invoices under this contract.

(PPR13) National Oceanic and Atmospheric Administration (NOAA) Grants Online (GOL)

Project Summary: Team CyberData provides O&M support for NOAA's grants management system, which has become the Department of Commerce standard. Responsibilities include applications management such as: release management and developing testing and implementing new features, help desk support for over 6,000 users, Oracle database administration, web-based work flow management and communications, and training. Team CyberData also supported the transition of users and data systems from other Commerce grants systems into Grants Online. We are performing a follow on contract to continue the same service.

Expanded description of work performed and results achieved: The original project entailed consolidation of NOAA's 12 disparate grant processing systems into an integrated grants management system with standard business processes. Working closely with the client, we delivered functionality incrementally over two iterations. We used Rapid Application Development as the software development lifecycle (SDLC) to deliver capabilities in advance of deployment. The resultant system reduces processing time by over 90%, provides consistent workflow and integrates with both the Federal Grant.gov portal and NOAA's financial management systems. Grants Online enabled the NOAA to become the first agency to receive an electronic application directly from Grants.gov.

Other accomplishments include transitioning grants systems of 5 other bureaus; establishment and operation of Tier 1, Tier 2 help desk, and upgrade of an obsolete middleware system to Oracle's WebLogic 11g. The WebLogic transition was completed ahead of schedule and at less than 50% of the Independent Government Estimate based on input from Oracle Professional Services. Team CyberData also provides the GOL Information System Technical Security Officer.

Description of methodology, tools, and processes utilized in performing the work: In accordance with our ISO 9001 certification, Team CyberData employs standardized processes for quality management, testing, and requirements management. Our development team uses, Ultra, a customized tool to help manage configuration change and assure requirements traceability. The Help Desk team employs the HEAT help desk management system to track tickets and problem resolution. The GOL application stack includes an IIS web server integrated with WebLogic, a SOA based Java development platform to perform workflow management and develop reports from the underlying Oracle database. Team CyberData employs Project Management Institute practices to manage and assure schedule compliance on GOL development projects such as the ongoing Review Module enhancement.

Adherence to project schedule and cost: All work was completed on schedule within the original resource allocation.

Problems encountered and corrective actions taken: In 2009 NOAA needed to upgrade GOL from an "End-of- Life" WebLogic 8.1 environment to WebLogic 11g. The upgrade involved a significant infrastructure change as well as a rewrite of workflow processes critical to grants management integrity. Due to the complications associated with the two version upgrade, NOAA attempted to contract with Oracle Professional Services, but was reluctant to commit to and expensive, unbounded Time and

Material rates. Team CyberData augmented our base staff with two consultants, who developed an alternate solution to enable NOAA to complete the transition for less than half of the original budget and within an aggressive time schedule.

Similarity in scope and complexity to this project: GOL includes many of the core services required by FOST including systems administration, database administration, web development, complex and sensitive data migration and integration, business analysis to, technical writing and testing.

(PPR14) NOAA/NWS Sterling Field Support Center

Team CyberData provides a diverse mix of meteorologists, electrical engineers, IT experts and engineers to manage and operate fully-equipped labs to test and evaluate weather systems and upper air sensor equipment and associated laboratory infrastructure. Team CyberData is responsible for the successful testing and validation of a wide range of operational NWS systems, including:

- Upper air radiosonde systems
- RRS software systems
- In-situ surface systems
- COTS Fisher Porter rebuild systems
- Cooperative Observer Program temperature sensors and other test equipment

(PPR15) NOAA Security Operation Center (SOC) Support

RCG provides support to the five operational pillars performed by a SOC: 1) security event generation; 2) data collection; 3) data storage; 4) analysis; and 5) reaction. RCG has provided these services for several government agencies, including the Department of Commerce and the Small Business Administration and currently provides these services for NOAA. RCG's mission is to provide risk management through centralized analysis using the combined resources consisting of personnel, dedicated hardware and specialized software.

RCG's solutions for security operations provide guidance and expertise as well as our knowledge of proven technology platforms to establish a security operations program. We provide the expertise to effectively identify, manage and report on information risk across an entire organization, and the necessary controls needed to adapt to the ever-changing landscape of compliance. Understanding that network, application and database vulnerabilities emerge every day, it is essential that these exposures are eliminated to protect your critical IT assets and safeguard sensitive information. RCG ensures that network security and response tools are articulated as part of the infrastructure design to minimize these risks.

RCG's security support has consisted of monitoring and analyzing systems, devices, applications, firewall activity, and intrusion detection and intrusion prevention systems, and ensuring antivirus/antispam is kept up to date and vulnerabilities are addressed. RCG has assisted in the planning and development of PKI policy, security system plans, processes and procedures and makes sure that updates are made when necessary.

RCG has establishes firewall policy and provides proactive firewall management to prevent unauthorized access and costly breaches. RCG supported firewall devices are provisioned, deployed, upgraded and patched to keep up with the latest threats.

RCG performs comprehensive security risk assessments and provides recommendations for securing customers systems, including those that are mission critical. We evaluate and assist with the selection of Intrusion Detection and Intrusion Prevention Systems. We monitor and manage network infrastructures, systems logs, proxy logs, and DNS logs for operational and security risks.

RCG performs expert signature tuning and device management to ensure maximum value out of devices. When the service or device is implemented, our experts conduct extensive base lining to tailor detection and alerting to the customer network.

RCG conducts vulnerability testing and identifies areas that need improvement in an effort to create a sustainable, enhance-able framework for advanced security operations. We conduct code auditing and perform vendor product evaluation for security risks prior to purchase of the product by our customers. RCG prides itself in being vendor agnostic and evaluates solutions based on bringing the right product and solution to our customers.

Index of Team Cyberdata's Past Performance References